

MAR 10 2006

PTO/SB/21 (09-04)


Approved for use through 07/31/2006. OMB 0551-0031

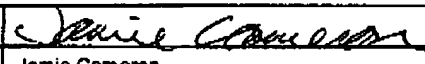
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	09/489,864	
	Confirmation Number	6357	
	Filing Date	01/24/2000	
	First Named Inventor	Allan L. Samson	
	Art Unit	2134	
Examiner Name		Michael J. Simitoski	
Total Number of Pages in This Submission	26	Attorney Docket Number	5010/097

ENCLOSURES (check all that apply)		
<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/ Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below):
Remarks It is believed that no fees are due in this matter. However, if it is determined that fees are due, the Commissioner is authorized to debit Deposit Account No. 502622 for the required fees.		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm	Setter Ollila LLC		
Signature			
Printed Name	Gregg L. Jansen		
Date	3/10/2006	Reg. No.	46,799

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO, fax number (571) 273-8300, addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.			
Signature			
Typed or printed name	Jamie Cameron	Date	3/10/2006

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER

MAR 10 2006

Setter Ollila LLC
2060 Broadway
Suite 300
Boulder, Colorado 80302

PATENT APPLICATION**ATTORNEY DOCKET NO. 35010/097****IN THE UNITED STATES PATENT AND TRADEMARK OFFICE****In re application of: Allan L. Samson et al.****Application No.: 09/489,864****Group No.: 2134****Filed: 01/24/2000****Examiner: Simitoski, Michael J.**

**For: SYSTEM FOR PREVENTING TAMPERING WITH SIGNAL CONDITIONER
REMOTE FROM A HOST SYSTEM**

**MAIL STOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P. O. Box 1450
Alexandria, VA 22313-1450**

AMENDED BRIEF ON APPEAL**INTRODUCTION**

Pursuant to the provisions of 37 CFR § 1.191 *et seq.*, Applicants hereby appeal to the Board of Patent Appeals and Interferences (the "Board") from the Examiner's final rejection dated May 6, 2004.

A notice of appeal was previously filed. An appeal brief was filed on November 1, 2004. A Notification of Non-Compliant Appeal Brief was mailed on April 5, 2005. An amended Appeal Brief was filed on April 13, 2005. An Order Returning Undocketed Appeal To Examiner was received by Applicants on March 1, 2006, specifying that the Appeal Brief was still non-compliant under 37 CFR § 41.37(c). Applicants herein supply a further Amended Appeal Brief fully complying with the Order.

This amended brief on appeal is being filed in compliance with 37 CFR § 41.37. The requisite fee was previously supplied with the originally filed Appeal Brief.

RECEIVED
CENTRAL FAX CENTER

MAR 10 2006

REAL PARTY IN INTEREST

The entire interest in the present application has been assigned to Micro Motion, Inc. as recorded at Reel 010522, Frame 0192.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-44 (all claims) are pending.

Claims 1-44 have been finally rejected.

Claims 1-44 are on appeal.

STATUS OF AMENDMENTS

There are pending amendments. Applicants filed a response after final on June 24, 2004, amending the claims. An Advisory Action dated August 18, 2004 was issued, with the Advisory Action maintaining the final rejection. In addition, the Advisory Action stated that the submitted claim amendments were not entered because the amendments would require further consideration and/or search and that the amendments did not place the application in better form for appeal. Applicants filed a response to the Advisory Action on September 7, 2004, stating that the submitted claim amendments did not require further consideration and/or search, as the submitted claim amendments did not differ significantly from the claims as originally filed.

SUMMARY OF CLAIMED SUBJECT MATTER

This invention relates generally to a system for preventing tampering with a signal conditioner 110 remote from a host system 100 (see FIG. 1 and page 6, lines 2-3 and lines 6-15). The signal conditioner 110 is circuitry that receives signals from sensors 605 and 605' (see FIG.

6) and converts the signals to parameter signals that indicate properties of a material (see page 3, lines 9-12). An example of a system parameter is a property of a material that the sensors 605 and 605' are detecting (see page 3, lines 31-32). The sensors 605 and 605' may be attached to any type of device (see page 5, lines 32-33).

The signal conditioner 110 stores some manner of authentication data, such as calibration and configuration data as well as a unique identification (see page 3, lines 15-20). The authentication data comprises data that generally does not change over time (see page 8, lines 2-4). Therefore, the authentication data can comprise one or more of the identification, calibration, and configuration data.

The host system 100 is a processing unit that executes applications which provide the tamper proof system in accordance with this invention (see page 3, lines 15-16). The host system 100 supplies power to the signal conditioner 110 and receives the parameter signals from the signal conditioner 110 (see FIG. 1 and page 3, lines 11-12).

In order to prevent tampering, the host system 100 periodically transmits a request to the signal conditioner 110 for authentication data of the signal conditioner 110 (see FIG. 3 and page 8, lines 1-24). The signal conditioner 110 receives the request and reads the authentication data. The authentication data is then transmitted to the host system 100. The host system 100 stores the received information in a memory to provide an audit trail. The host system 100 may also compare the received authentication information to initial authentication information stored in the host system 100. If the current authentication data does not match the initial information, the host system 100 may generate an error signal. The error signal indicates possible tampering, or can indicate some other type of error. In response to the error signal, the host system 100 may disable the system and/or cease operation of the system. The ceasing of operation prevents any potentially false reading from being used, such as false, corrupted, or improperly calibrated parameter signals.

The authentication information can be checked periodically to insure against tampering. Periodically means that the process may be executed at a set time interval, after a batch of a predetermined number of measurements are taken, or at random time intervals (see page 7, lines 29-32).

The host system 100 can obtain the initial information in the following manner. The host

system 100 transmits an initialize request to the signal conditioning circuitry for the authentication information in response to detecting a signal conditioning circuitry being connected to the host system 100 (see FIG. 5 and page 9, lines 3-12). The host system 100 then receives the authentication information from the signal conditioning circuitry and stores the authentication information as the initial information in the memory. The record of the authentication information can include a time stamp indicating when the authentication information is received (see page 5, lines 3-4).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1, 12, 23, and 34 comply with the written description requirement under 35 U.S.C. § 112, first paragraph.
2. Whether claims 1, 12, 23, and 34 are indefinite under 35 U.S.C. § 112, second paragraph.
3. Whether claims 1-3, 8, 9, 34-36, 41, and 43 are anticipated under 35 U.S.C. § 102(b) over U.S. Patent 4,388,690 (Lumsden).
4. Whether dependent claims 4-7, 10-12, 15-18, 21-23, 26-29, 32, 33, 37-40, 42, and 44 are obvious under 35 U.S.C. § 103(a) over U.S. Patent 4,388,690 (Lumsden) in view of various combinations of Leigh-Monstevens et al., Barger et al., Sipin et al., Kuo et al., and Oyer.

ARGUMENT

OUTLINE

- I. Summary of the brief on appeal.
- II. Summary of the requirements for *prima facie* anticipation and obviousness.
- III. Discussion of the § 112, first paragraph rejection of claims 1, 12, 23, and 34.
- IV. Discussion of the § 112, second paragraph rejection of claims 1, 12, 23, and 34.

- V. Discussion of the § 102(b) anticipation rejection of claims 1-3, 8, 9, 34-36, 41, and 43.
- VI. Discussion of the various § 103(a) obviousness rejections of claims 4-7, 10-12, 15-18, 21-23, 26-29, 32, 33, 37-40, 42, and 44.

I. Summary of the brief on appeal

- A. The 35 U.S.C. § 112, first paragraph rejection of claims 1, 12, 23, and 34 is improper because the signaling was fully disclosed in the application as originally filed.
- B. The 35 U.S.C. § 112, second paragraph rejection of claims 1, 12, 23, and 34 is improper because the signaling is particularly and distinctly described in the application as filed.
- C. The 35 U.S.C. § 102(b) rejection of claims 1-3, 8, 9, 34-36, 41, and 43 is improper because a *prima facie* case for anticipation has not been established, for the following reasons: (1) the cited Lumsden reference does not teach or suggest every element of the claims, and (2) the Examiner incorrectly characterizes the Lumsden reference.
- D. The 35 U.S.C. § 103(a) rejection of claims 4-7, 10-12, 15-18, 21-23, 26-29, 32, 33, 37-40, 42, and 44 is improper because a *prima facie* case for obviousness has not been established, for the following reasons: (1) the cited prior art combination does not teach or suggest every element of the claims, and (2) the Examiner incorrectly characterizes the Lumsden reference.

II. Summary of the requirements for *prima facie* indefiniteness, anticipation, and obviousness.

The Court of Appeals for the Federal Circuit has held that "The test for determining compliance with the written description requirement is whether the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter, rather than the presence or absence of literal support in the specification for the claim language." *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1089 (Fed. Cir. 1983) quoting *In re Edwards*, 558 [568] F.2d 1349, 196 USPQ 465 (CCPA 1978); *In re Herschler*, 591 F.2d 693, 200 USPQ 711 (CCPA 1979).

The Court of Appeals for the Federal Circuit has held that "The operative standard for determining whether this [definiteness] requirement has been met is 'whether those skilled in the art would understand what is claimed when the claim is read in light of the specification.'" *Beachcombers, Int'l, Inc. v. WildeWood Creative Products, Inc.*, 31 F.3d 1154, 31 USPQ2d 1653 (Fed. Cir. 1994).

The all elements rule for anticipation is well established over a long series of case law. The all elements rule states that for anticipation to exist, a single anticipating prior art reference must include all elements of a claim. *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 231 USPQ 81 (Fed. Cir. 1986). "When the defense of lack of novelty is based on a printed publication that is asserted to describe the same invention, a finding of anticipation requires that the publication describe all of the elements of the claims, arranged as in the patented device." *C.R. Bard, Inc. v. M3 Systems, Inc.*, 157 F.3d 1340, 48 USPQ2d 1225 (Fed. Cir. 1998), *rehearing denied & suggestion for rehearing en banc declined*, 161 F.3d 1380 (Fed. Cir. 1998).

Anticipation under Section 102 can be found only if a reference shows exactly what is claimed; where there are differences between the reference disclosures and the claim, a rejection must be based on obviousness under Section 103. *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985).

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2142. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim dependent therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

III. Discussion of the § 112, first paragraph rejection of claims 1, 12, 23, and 34.

Independent claims 1, 12, 23, and 34 have been finally rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. The Office Action asserts that the limitation that the host signals a tamper condition in the signal conditioning circuitry was not disclosed in the patent application. Applicants contend that the signaling was fully disclosed and point to FIGS. 1 and 3 and the accompanying text at page 6, lines 6-30 and page 7, line 25 through page 8, line 24. Applicants also point to page 1, lines 4-10.

IV. Discussion of the § 112, second paragraph rejection of claims 1, 12, 23, and 34.

Independent claims 1, 12, 23, and 34 have been finally rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. The Office Action asserts that it is unclear how the host will "signal" a tampering condition "in the signal conditioning circuitry". This is a straightforward process known in the art, wherein the host system receives the authentication information, performs the comparison, and signals the error condition. The error condition indicates tampering in the signal conditioning circuitry. The error condition signal can be generated and held in the host system in order to signal an error condition in the signal conditioning circuitry. Error condition signals generated by a host system can be available for inspection by an operator or technician, for example. In addition, the error condition can be transmitted to other devices.

V. Discussion of the § 102(b) anticipation rejection of claims 1-3, 8, 9, 34-36, 41, and 43.

Claims 1-3, 8, 9, 34-36, 41, and 43 have been finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 4,388,690 (Lumsden).

Independent claims 1, 12, 23, and 34 each require periodically transmitting a request for authentication information from a host system to a signal conditioner, receiving the authentication information from the signal conditioning circuitry in response to the request, comparing the authentication information with initial information, and signaling a tampering condition in the signal conditioning circuitry in response to the authentication information not being equal to the initial information. Advantageously, the invention provides a system for detecting tampering with a signal conditioning circuitry that is remote from a host system.

The authentication information can include identification, calibration, and configuration data (see page 3, lines 16-20). The initial information comprises authentication information received from the signal conditioning circuitry in response to detecting the signal conditioning circuitry being connected to the host system (see page 4, lines 20-26). The initial information therefore can comprise an initial version of the authentication information (*i.e.*, it is the first set of authentication information received from the signal conditioning circuitry).

Lumsden discloses a system for reporting electrical power usage from a residential power meter to a central computer (see abstract). Lumsden provides a transponder that acts as a simple storage device for utility data. The transponder receives data from a data source and stores it until such data is requested through an external instruction (see col. 3, lines 34-59). Lumsden discloses that the central computer sends commands to these residential power meters over telephone lines (see col. 2, lines 56-59). The commands can specify that a particular meter report its stored power consumption data (see col. 2, lines 21-24). Lumsden also discloses requesting information concerning a load of a particular user and subsequent actions to alleviate excessive loads to that user (see col. 4, lines 44-59). Multiple meters in Lumsden can communicate over a single telephone line. Therefore, a particular power meter is identified by a unique code stored in that meter (see col. 2, lines 48-56), *i.e.*, a message is broadcast by the central computer, but only the transponder specified by an ID code in the broadcast message receives and acts on the message.

Lumsden does not teach or suggest signaling an error condition that indicates tampering in the signal conditioning circuitry, with the signaling being in response to the authentication information not being equal to the initial information. The Office Action implies that Lumsden performs some manner of tampering detection by asserting that the "central computer can send a load shed command/alarm/tampering condition to the transponder." This is incorrect.

Lumsden does not disclose any comparison of received authentication information to initial information. Lumsden does not disclose any signaling of an error condition if the authentication information is not equal to the initial information. Lumsden discloses two comparison operations. First, Lumsden discloses that the central computer monitors electrical power usage measurements and compares these electrical power usage measurements to predetermined electrical power consumption levels (see col. 1, lines 35-38). Second, Lumsden compares transponder identification codes to known codes in order to regulate electronic communications and identify message transmitters and message recipients. Therefore, the Office Action improperly implies tampering detection in Lumsden when all Lumsden discloses is comparing customer electrical power usage to a predetermined level in order for the central computer of Lumsden to perform load shedding actions.

The Examiner appears to be equating the initial authentication information of the invention with the electrical power consumption threshold of Lumsden. This is incorrect. The threshold of Lumsden would have to be an electrical power consumption level, and not authentication information as given in the present application.

Lumsden does not teach or suggest requesting or receiving authentication information as in the present application. While Lumsden includes a transponder identification code in communication messages, the transponder identification code does not comprise authentication data as in the present application. In addition, Lumsden discloses that the transponder identification code is hard-wired into the transponder (see col. 2, lines 48-50). The term "hard-wired" connotes physical provision or formation of digital data, wherein the digital data is not programmed into a memory but is provided as a digital voltage level and therefore cannot be tampered with and cannot be changed. The hard-wired transponder identification code of Lumsden cannot be reprogrammed and therefore cannot be used for detecting tampering.

Independent claims 1, 12, 23, and 34 therefore include features that are neither taught nor suggested by Lumsden. It is respectfully submitted that a *prima facie* case of anticipation has not been established. As a result, independent claims 1, 12, 23, and 34 are allowable as written.

Claims 2-3, 8-9, 35-36, 41, and 43 are dependent on claims 1, 12, 23, and 34. If an independent claim is patentable under 35 U.S.C. 102, then any claim dependent therefrom is also patentable, as a dependent claim includes all of the elements and limitations of the corresponding independent claim.

VI. Discussion of the § 103(a) obviousness rejections of claims 4-7, 10-12, 15-18, 21-23, 26-29, 32, 33, 37-40, 42, and 44.

Dependent claims 5 and 38 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 5,014,038 (Leigh-Monstevens et al.). Dependent claims 5 and 38 depend from independent claims 1 and 34 and therefore incorporate the limitations of the independent claim. Consequently, claims 5 and 38 are patentable for the reasons previously discussed. To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2142. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim dependent therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Dependent claims 4, 10, 11, 37, 42, and 44 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 6,289,456 (Kuo et al.). Dependent claims 4, 10, 11, 37, 42, and 44 depend from independent claims 1 and 35 and therefore incorporate the limitations of the independent claim. Consequently, claims 4, 10, 11, 37, 42, and 44 are patentable for the reasons previously discussed.

Dependent claims 6 and 7 have been finally rejected under 35 U.S.C. § 103(a) as being

obvious over Lumsden in view of U.S. Patent 4,933,668 (Oyer). Dependent claims 6 and 7 depend from independent claim 1 and therefore incorporate the limitations of the independent claim. Consequently, claims 6 and 7 are patentable for the reasons previously discussed.

Dependent claims 39 and 40 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Leigh-Monstevens and Oyer. Dependent claims 39 and 40 depend from independent claim 34 and therefore incorporate the limitations of the independent claim. Consequently, claims 39 and 40 are patentable for the reasons previously discussed.

Claims 12-14, 19-20, 23-25, 30, and 31 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 6,526,839 (Barger et al.) and further in view of U.S. Patent 3,355,944 (Sipin). The rejection reiterates the assertion that Lumsden discloses a meter system as in the present invention, but lacks disclosure of meter electronics for a Coriolis flowmeter. This is incorrect. As previously discussed, Lumsden does not disclose comparing an authentication information to an initial information and does not disclose signaling an error condition. Therefore, the combination of Lumsden, Barger, and Sipin does not provide a system that detects an error. The combination of Lumsden, Barger, and Sipin does not render obvious independent claims 12 and 23. Claims 13-14, 19-20, 24-25, 30, and 31 all depend from independent claims 12 and 23 and therefore incorporate the limitations of the independent claims. Consequently, claims 13-14, 19-20, 24-25, 30, and 31 are patentable as discussed above. To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2142. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim dependent therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Dependent claims 16 and 27 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Barger, Sipin, and Leigh-Monstevens. Dependent claims 16 and 27 depend from independent claims 12 and 21 and therefore incorporate the limitations of the independent claim. Consequently, claims 16 and 27 are patentable for the reasons previously

discussed.

Claims 15, 21, 22, 26, 32, and 33 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Barger, Sipin, and Kuo. As previously discussed, Lumsden does not disclose comparing an authentication information to an initial information and does not disclose signaling an error condition. Therefore, the combination of Lumsden, Barger, Sipin, and Kuo does not provide a system that detects an error. The combination of Lumsden, Barger, Sipin, and Kuo does not render obvious independent claim 21. Dependent claims 15, 22, 26, 32, and 33 depend from independent claims 12 and 21 and therefore incorporate the limitations of the independent claim. Consequently, claims 15, 21, 22, 26, 32, and 33 are patentable for the reasons previously discussed.

Dependent claims 17 and 18 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Barger, Sipin, Leigh-Monstevens, and Oyer. Dependent claims 17 and 18 depend from independent claim 12 and therefore incorporate the limitations of the independent claim. Consequently, claims 17 and 18 are patentable for the reasons previously discussed.

Dependent claims 28 and 29 have been finally rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Barger in view of Sipin and further in view of Oyer. Dependent claims 28 and 29 depend from independent claim 21 and therefore incorporate the limitations of the independent claim. Consequently, claims 28 and 29 are patentable for the reasons previously discussed.

Conclusion

In view of the above, applicant respectfully request that the examiner's rejection of claims 1-44 be reversed.

Respectfully submitted,

Date: 3/10/06


SIGNATURE OF PRACTITIONER

Gregg Jansen, Reg. No. 46,799
Setter Ollila LLC
Telephone: (303) 938-9999 ext. 14
Facsimile: (303) 938-9995

Correspondence Address:

Customer No: 32827

CLAIMS APPENDIX

1. A system for preventing-tampering with signal conditioning circuitry in electronics that determines a parameter from signals received from sensors, said system comprising:

a host system that receives data from and sends data to said signal conditioning circuitry;

a processing unit in said host system;

a memory connected to said processing unit;

instructions for directing said processing unit in said host system to periodically transmit a request for authentication information from said signal conditioning circuitry, receive said authentication information from said signal conditioning circuitry in response to said request, comparing said authentication information with initial information, and signal a tampering condition in the signal conditioning circuitry in response to said authentication information not being equal to said initial information; and

a media readable by said processing unit for storing said instructions.

2. The system of claim 1 wherein said authentication information includes a unique identification for said signal conditioning circuitry.

3. The system of claim 1 wherein said authentication information includes calibration data for said signal conditioning circuitry.

4. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to store a record of said authentication information received from said signal conditioning circuitry in said memory.

5. The system of claim 1 wherein said instructions for directing said processing

unit in said host system includes:

instructions for directing said processing unit in said host system to terminate operation of said system.

6. The system of claim 1 wherein said instructions include:

instructions for directing said processing unit to obtain said initial information.

7. The system of claim 6 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:
transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,
receive said authentication information from said signal conditioning circuitry, and
store said authentication information as said initial information in said memory.

8. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to compare said authentication information with initial information, and perform a programmed function in response to said authentication information not being equal to said initial information.

9. The system of claim 1 further comprising:

a processing unit in said signal conditioning circuitry;

a memory connected in said signal conditioning circuitry that stores said authentication information;

instructions for directing said processing unit in said signal conditioning circuitry to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioning circuitry for storing said instructions.

10. The system of claim 4 wherein said record includes a time stamp indicating when said authentication information is received.

11. The system of claim 4 wherein said record includes said authentication information received from said signal conditioning circuitry.

12. Meter electronics for a Coriolis flowmeter that detects possible tampering comprising:

a host system that receives parameter signals indicating properties of a material flowing through said Coriolis flowmeter from said signal conditioner and supplies power to signal conditioner;

a signal conditioner remote from said host system and communicatively connected to said host system wherein said signal conditioner receives pick-off signals from sensors affixed to said Coriolis flowmeter and generates said parameter signals from said pick-off signals;

a processing unit in said host system;

a memory connected to said processing unit in said host system;

instructions for directing said processing unit in said host system to:

periodically transmit a request for authentication information to said signal conditioner,

receive said authentication information from said signal conditioner in response to said request,

compare said authentication information with initial information, and

signal a tampering condition in the signal conditioning circuitry in response to said authentication information not being equal to said initial information; and

a media readable by said processing unit for storing said instructions.

13. The meter electronics of claim 12 wherein said authentication information includes a unique identification for said signal conditioner.

14. The meter electronics of claim 12 wherein said authentication information includes calibration data for said signal conditioner.

15. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for storing a record of said authentication information in said memory.

16. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes;

instructions for directing said processing unit in said host system to terminate operation of said system.

17. The meter electronics of claim 16 wherein said instructions include:

instructions for directing said processing unit to obtain said initial information.

18. The meter electronics of claim 17 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:

transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,

receive said authentication information from said signal conditioning circuitry, and

store said authentication information as said initial information in said memory.

19. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and perform a programmed function in response to said authentication information not being equal to said initial information.

20. The meter electronics of claim 12 further comprising:

a processing unit in said signal conditioner;

a memory connected in said signal conditioner that stores said authentication information;

instructions for directing said processing unit in said signal conditioner to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioner for storing said instructions.

21. The meter electronics of claim 15 wherein said record includes a time stamp indicating when said authentication information is received.

22. The meter electronics of claim 15 wherein said record includes said authentication information received from said signal conditioner.

23. A Coriolis flowmeter having tamper resistant meter electronics comprising:

- at least one flow tube through which material flows;
- a driver affixed to said at least one flow tube that vibrates said at least one flow tube as said material flows through said at least one flow tube;
- sensors affixed to at least two different points of said at least one flow tube to generate sensor signals indicating vibrations of said at least one flow tube at said at least two different points;
- a signal conditioner that transmits a drive signal to said driver, receives said sensors signals, and generates parameter signals from said sensors signals wherein said parameter signals indicate a property of said material;
- a host system that provides power to said signal conditioner and receives said parameter signals from said signal conditioner;
- a processing unit in said host system;
- a memory connected to said processing unit in said host system;
- instructions for directing said processing unit in said host system to:
 - periodically transmit a request for authentication information to said signal conditioner,
 - receive said authentication information from said signal conditioner in response to said request,
 - compare said authentication information with initial information, and
 - signal a tampering condition in the signal conditioning circuitry in response to said authentication information not being equal to said initial information; and
- a media readable by said processing unit for storing said instructions.

24. The Coriolis flowmeter of claim 23 wherein said authentication information includes a unique identification for said signal conditioner.

25. The Coriolis flowmeter of claim 23 wherein said authentication information includes calibration data for said signal conditioner.

26. The Coriolis flowmeter of claim 23 wherein said instruction for directing said processing unit in said host system includes:
instructions for storing a record of said authentication information in said memory.

27. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:
instructions for directing said processing unit in said host system to terminate operation of said Coriolis flowmeter in response to said signal.

28. The Coriolis flowmeter of claim 27 wherein said instructions for directing said host system include:
instructions for directing said processing unit to obtain said initial information.

29. The Coriolis flowmeter of claim 28 wherein said instructions for directing said processing unit to obtain said initial information includes:
instructions for directing said processing unit in said host system to:
transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,
receive said authentication information from said signal conditioning circuitry, and
store said authentication information as said initial information in said memory.

30. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and
perform a programmed function in response to said authentication information
not being equal to said initial information.

31. The Coriolis flowmeter of claim 23 further comprising:

a processing unit in said signal conditioner;

a memory connected in said signal conditioner that stores said authentication
information;

instructions for directing said processing unit in said signal conditioner to receive
said request for said authentication information, read said authentication information
from said memory, and transmit said authentication information to said host system;
and

a media readable by said processing unit in said signal conditioner for storing
said instructions.

32. The Coriolis flowmeter of claim 26 wherein said record includes a time
stamp indicating when said authentication information is received.

33. The Coriolis flowmeter of claim 26 wherein said record includes said
authentication information received from said signal conditioner.

34. A method for preventing tampering with signal conditioning circuitry in a system comprising the steps of:
periodically transmitting a request for authentication information from a host system to said signal conditioner;
receiving said authentication information from said signal conditioning circuitry in response to said request;
comparing said authentication information with initial information; and
signaling a tampering condition in the signal conditioning circuitry in response to said authentication information not being equal to said initial information.

35. The method of claim 34 wherein said authentication information includes a unique identification for said signal conditioning circuitry.

36. The method of claim 34 wherein said authentication information includes calibration data for said signal conditioner.

37. The method of claim 34 further comprising the steps of:
storing a record of said authentication information in a memory in said host system.

38. The method of claim 34 further comprising the steps of:
terminating operation of said system in response to said signal error.

39. The method of claim 38 further comprises the step of:
obtaining said initial information.

40. The method of claim 39 wherein said step of obtaining said initial information comprises the steps of:

transmitting a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system;

receiving said authentication information from said signal conditioning circuitry;
and

storing said authentication information as said initial information in said memory.

41. The method of claim 34 further comprising the steps of:

receiving said request for said authentication information in said signal conditioning circuitry;

reading said authentication information from a memory in said signal conditioning circuitry; and

transmitting said authentication information to said host system.

42. The method of claim 37 wherein said record includes a time stamp indicating when said authentication information is received.

43. The method of claim 34 further comprises the steps of:

comparing said authentication information with initial information stored in said host system; and

performing a programmed function in response to said authentication information not being equal to said initial information.

44. The method of claim 37 wherein said record includes said authentication information received from said signal conditioner.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None